Date of Publication
February 6, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Actors, Attacks, and Vulnerabilities

30 JANUARY to 5 FEBRUARY 2023

Summary

Threat Actors

Hive Pro discovered **four** actors that have been active in the past week. The first, **Sandworm Team**, is a well-known Russian threat actor known for Sabotage and destruction. The second, **UNC2565**, is an unknown threat group that specializes in Information theft and espionage. The third, **BlueBravo**, is a well-known Russian threat group known for Information theft and espionage. The fourth, **Lazarus Group**, is a well-known North Korean threat group known for Sabotage and destruction. For further details, see the key takeaway section for Actors.

Attacks

We also discovered **nine** new malware strains that have been active over the past week. The Ukrainian National Information Agency 'Ukrinform' was targeted by the Sandworm team in a partially successful cyber attack with **5 types of malicious malware**. The UNC2565 group is responsible for the **GOOTLOADER** malware, which infects systems via the download of a malicious archive. The Russian-linked threat group BlueBravo utilizes **GraphicalNeutrino and BEATDROP** as malicious software in targeted cyber attacks. To evade detection, the group employs legitimate Western services for C2 communications. **TrickGate** is a well-known Packer-as-a-Service that has successfully eluded detection from cybersecurity measures for over six years. The newly discovered **HeadCrab** malware, targeting vulnerable Redis servers online, has infected over 1,000 servers since September 2021. **VectorStealer** is malicious software that steals .rdp files by phishing emails, costing USD 63 in Bitcoin. Hackers have aimed at online gaming and gambling companies using an undetected **Ice Breaker** backdoor. A cluster of virtualized .NET malware loaders, referred to as **MalVirt**, is being spread through malvertising attacks. A new type of ransomware called **Nevada Ransomware** has been discovered with an affiliate program. For further details, see the key takeaway section for Attacks.

Vulnerabilities

Last week, we discovered **six** vulnerabilities that organizations should prioritize. **One** vulnerability was a security flaw in QNAP NAS devices, **one** critical vulnerability was found in the Windows CryptoAPI and **four** flaws were exploited by Lazarus Group For further details, see the key takeaway section on vulnerabilities.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Threat Actors

Sandworm Team (CaddyWiper, ZeroWipe, SDelete, AwfulShred, and BidSwipe.)
The Sandworm Team is a well-known Russian threat actor that conducted a cyber attack on Ukrinform on January 17th, 2023. However, the attack was only partially successful and only affected several data storage systems. The group is known for its destructive activities, as highlighted on the Telegram channel 'CyberArmyofRussia_Reborn,' which focuses solely on their destructive activities, including DDoS attacks and website defacements.

UNC2565 (GOOTLOADER)
The malware and infrastructure are attributed solely to the group UNC2565, and it is believed to be unique to this group. In 2022, UNC2565 made changes to their tactics, techniques, and procedures, such as using multiple versions of the FONELAUNCH launcher, distributing new follow-on payloads, and modifying the GOOTLOADER downloader and infection chain, including the addition of GOOTLOADER.POWERSHELL.

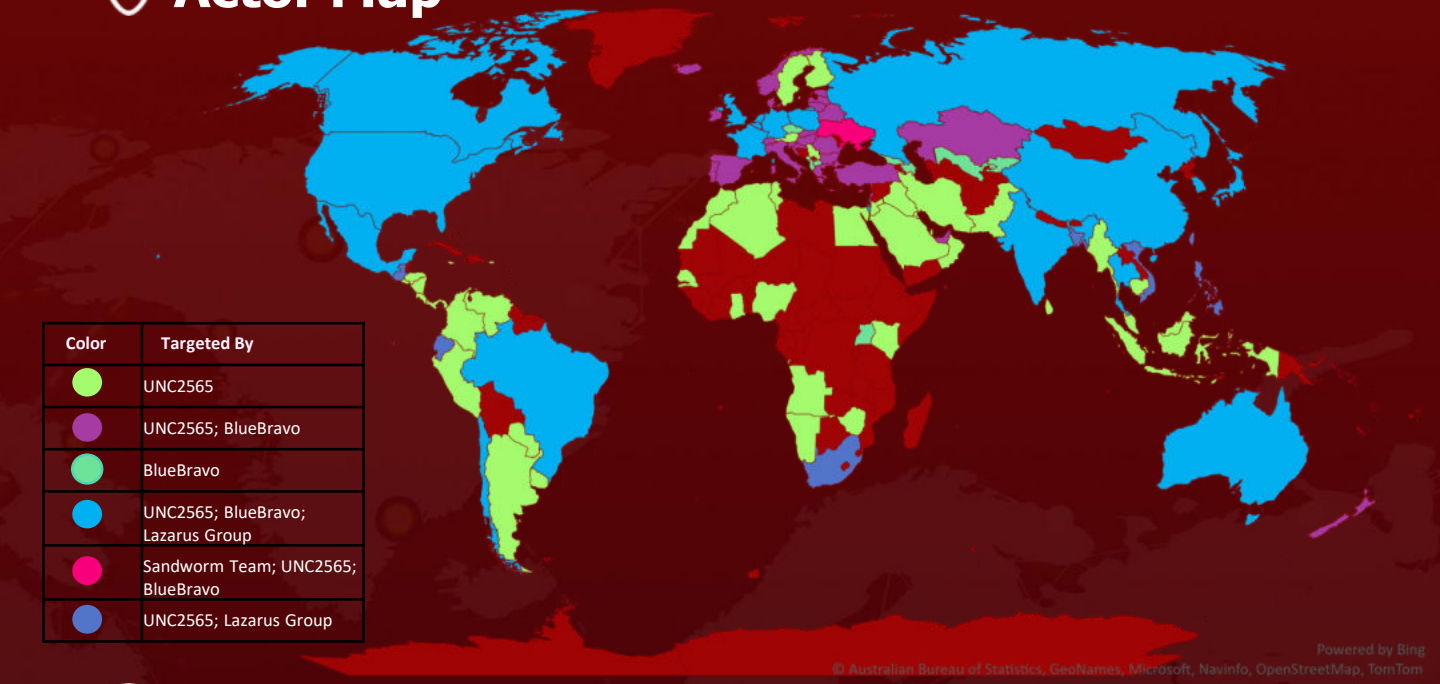
BlueBravo (GraphicalNeutrino and BEATDROP)
BlueBravo, a newly discovered threat group, is believed to have links to the Russian advanced persistent threat (APT) activities APT29 and NOBELIUM, both of which are associated with Russia's Foreign Intelligence Service (SVR). In October 2022, BlueBravo was found to use the GraphicalNeutrino malware, delivered through a malicious ZIP file. The targeted victims appear to be embassy personnel or an ambassador, as indicated by a website hack with the message “Ambassador's schedule November 2022”.

Lazarus Group (unattributed)
During the fourth quarter of 2022, the North Korean state-sponsored Lazarus Group carried out a cyber-attack targeting public and private sector research organizations and their supply chains for intelligence purposes. The attack utilized known vulnerabilities in unpatched Zimbra devices and employed off-the-shelf webshells, custom binaries, and abused legitimate Windows and Unix tools. Over 100GB of data was extracted from the network.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Actor Map



Color	Targeted By
	UNC2565
	UNC2565; BlueBravo
	BlueBravo
	UNC2565; BlueBravo; Lazarus Group
	Sandworm Team; UNC2565; BlueBravo
	UNC2565; Lazarus Group

Actor Details

ICON	NAME	ORIGIN	MOTIVE
	Sandworm Team (Sandworm,Iron Viking,CTG-7263,Voodoo Bear,Quedagh,TEMP.Noble,ATK 14,BE2,UAC-0082,UAC-0113)	Russia	Sabotage and destruction
	UNC2565	Unknown	Information theft and espionage
	BlueBravo(APT 29, Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa)	Russia	Information theft and espionage
	Lazarus Group(LABYRINTH CHOLLIMA, Group 77, HastatiGroup, WhoisHacking Team, NewRomanicCyber Army Team, Zinc, Hidden Cobra, Appleworm,APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace ,Gods Apostles ,Gods Disciples)	North Korea	Sabotage and destruction

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Attacks

CaddyWiper, ZeroWipe, SDelete, AwfulShred, and BidSwipe (Sandworm Team)
The Sandworm group, associated with the Russian Federation, initiated an attack on January 17th, 2023, using five malicious programs: CaddyWiper, ZeroWipe, SDelete, AwfulShred, and BidSwipe. The attackers aimed to disrupt the normal operation of users' computers, but their efforts were unsuccessful.

GOOTLOADER (UNC2565)
The GOOTLOADER infections have been active since late 2020 and are believed to be exclusively carried out by the UNC2565 group. The malware is spread through a malicious archive that contains a JavaScript file, known as GOOTLOADER, which downloads further payloads such as FONELAUNCH and either CobaltStrike BEACON or SNOWCONE and saves them in the registry. These payloads are executed via PowerShell in subsequent stages.

GraphicalNeutrino and BEATDROP (BlueBravo)
The BEATDROP malware is utilized for command-and-control (C2) communication, while GraphicalNeutrino employs Notion, a US business automation service, for its C2 purposes. The utilization of reputable Western services by BlueBravo to blend its malware traffic enhances its ability to evade detection. Given BlueBravo's tactics, techniques, and procedures, which align with the focus of APT29 and NOBELIUM on foreign espionage, active measures, and electronic surveillance, countries associated with the ongoing conflict in Ukraine face a heightened risk of being targeted.

TrickGate (unattributed)
TrickGate has integrated numerous of the most highly regarded top-distributed malware families, including Trickbot, Maze, Emotet, REvil, CoinMiner, CobaltStrike, Formbook, Remcos, AgentTesla, and many others. Despite its elusive reputation, it has continuously enhanced its capabilities and is now utilized to spread a vast array of harmful tools, including ransomware, remote access trojans (RATs), information stealers, bankers, and miners.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

HeadCrab (unattributed)

HeadCrab is a novel and potent malware that is penetrating and residing on servers globally. This custom-made Redis-based malware is evading detection by conventional antivirus solutions and has already compromised over 1,200 Redis servers. The attack begins when the attacker designates a Redis server as a slave and downloads the HeadCrab malware, a malicious Redis module, onto it.

VectorStealer (unattributed)

VectorStealer is a malicious software capable of purloining .rdp files, offering attackers the chance to execute RDP hijacking through unauthorized access to a victim's system. The VectorStealer operator primarily operates through a web interface and Telegram channel, and the malware can be created for USD 63 in Bitcoin using the web interface. The stolen information can be exfiltrated using SMTP, Discord, or Telegram.

Ice Breaker (unattributed)

Online gaming and gambling companies have been targeted by hackers using unseen backdoors, collectively referred to as Ice Breaker. The attacks make use of cunning social engineering strategies to install a JavaScript backdoor, and the link offered retrieves either an LNK payload or a VBScript file as a backup option.

MalVirt (unattributed)

MalVirt refers to a group of virtualized .NET malware loaders that are being circulated via malvertising attacks. The loaders employ obfuscated virtualization and the Windows Process Explorer driver to dodge anti-analysis and stop processes. The distributed malware belongs to the Formbook family and is part of a persistent campaign.

Nevada Ransomware (unattributed)

Nevada Ransomware is a Rust-based locker that can be controlled through a console using predefined flags and features an affiliate program. It was first announced on the RAMP underground community. The ransomware has been upgraded and its functionality improved for Windows and Linux/ESXi systems, with updated builds being made available to affiliates.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

TOP MITRE ATT&CK TTPS:

T1027 Obfuscated Files or Information	**T1071** Application Layer Protocol	**T1082** System Information Discovery	**T1059** Command and Scripting Interpreter	**T1036** Masquerading
T1057 Process Discovery	**T1204** User Execution	**T1518** Software Discovery	**T1055** Process Injection	**T1574** Hijack Execution Flow
T1547 Boot or Logon Autostart Execution	**T1071.001** Web Protocols	**T1129** Shared Modules	**T1566** Phishing	**T1033** System Owner/User Discovery
T1218 System Binary Proxy Execution	**T1036.005** Match Legitimate Name or Location	**T1562** Impair Defenses	**T1018** Remote System Discovery	**T1204.002** Malicious File
T1083 File and Directory Discovery	**T1543** Create or Modify System Process	**T1087** Account Discovery	**T1547.001** Registry Run Keys / Startup Folder	**T1105** Ingress Tool Transfer
T1562.001 Disable or Modify Tools	**T1140** Deobfuscate/ Decode Files or Information	**T1569** System Services	**T1574.002** DLL Side-Loading	**T1190** Exploit Public-Facing Application
T1564 Hide Artifacts	**T1553** Subvert Trust Controls	**T1574.001** DLL Search Order Hijacking	**T1016** System Network Configuration Discovery	**T1090** Proxy

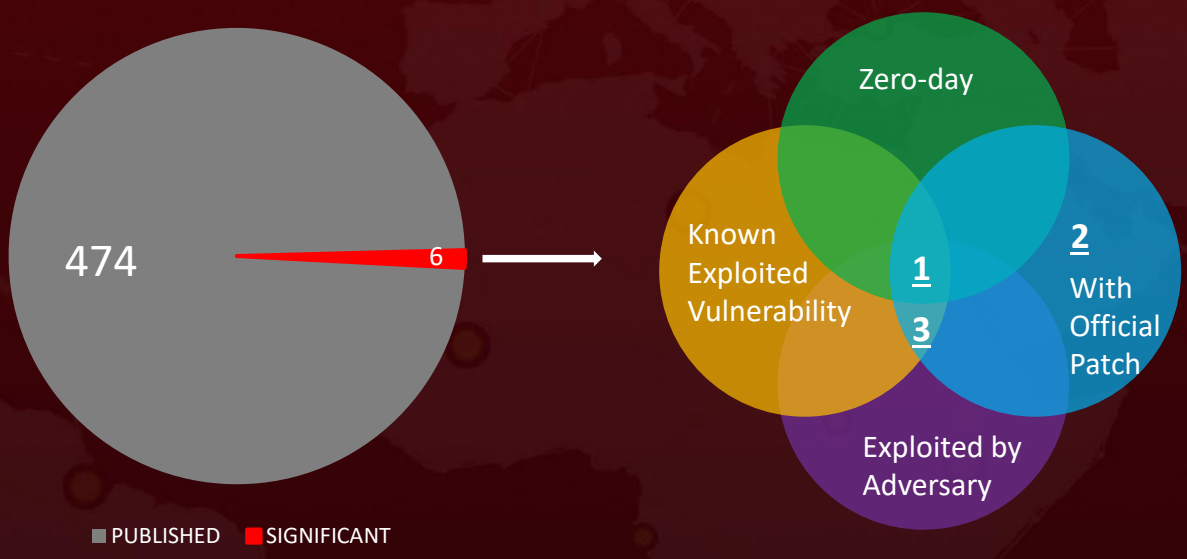
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

One Zero-day and Five Notable Mentions

Among these six vulnerabilities, one was found in QNAP network-attached storage (NAS) devices, allowing for arbitrary code injection. This vulnerability enables a remote attacker to execute any SQL query on the database and has been designated as CVE-2022-27596. CVE-2022-34689 is a critical vulnerability in the Windows CryptoAPI that was publicly disclosed by Microsoft in October 2022. The vulnerability enables an attacker to impersonate a trustworthy entity by exploiting the belief that the certificate cache index key, which is based on MD5, is free of collisions. The Lazarus Group exploited four vulnerabilities in their cyber attack against public and private sector research organizations and their supply chains for intelligence gathering. The attack used known vulnerabilities in unpatched Zimbra devices to gain initial access and escalate privileges. The actors also leveraged multiple proxy addresses to install commodity webshells and tunneling/relay software. They then exploited a local privilege escalation vulnerability (PwnKit) and an Out-of-Bounds Read and Write Vulnerability in Red Hat Polkit. Additionally, they used a **zero-day in Windows Print Spooler** called PrintNightmare, which led to a Remote Code Execution flaw.



*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **six significant vulnerabilities** and block the indicators related to the threat actor **Sandworm Team**, **UNC2565**, **BlueBravo**, **Lazarus Group** and malware **CaddyWiper**, **ZeroWipe**, **SDelete**, **AwfulShred**, **BidSwipe**, **GOOTLOADER**, **GraphicalNeutrino**, **BEATDROP**, **TrickGate**, **HeadCrab**, **VectorStealer**, **Ice Breaker**, **MalVirt**, and **Nevada ransomware**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **six significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to malware **CaddyWiper**, **ZeroWipe**, **SDelete**, **AwfulShred**, **BidSwipe**, **GOOTLOADER**, **GraphicalNeutrino**, **BEATDROP**, **TrickGate**, **HeadCrab**, **VectorStealer**, **Ice Breaker**, **MalVirt**, and **Nevada ransomware** in Breach and Attack Simulation(BAS).

Threat Advisories

Check out the links below for more extensive remediation and security precautions

Cyber Attack on Ukrainian National Information Agency

QNAP addresses a vulnerability in NAS devices

Proof-of-concept released for Windows CryptoAPI vulnerability

Infection and Evolution of the GOOTLOADER Malware

Uncovering the Threat of BlueBravo with GraphicalNeutrino and BEATDROP

The Menace of TrickGate Packer-as-a-Service Spreading Malware Globally

Headcrab malware is targeting Redis servers worldwide to mine Monero

VectorStealer Malware steals Sensitive Information via RDP Hijacking and Phishing Attacks

Ice Breaker a Looming Threat on the Gaming Industry

MalVirt: .NET Malware Loaders Spread through Malvertising Attacks

Unveiling the Advanced Rust-based Nevada Ransomware

Cyberattack on Medical and Energy Sector by Lazarus Group

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**:Threat Exposure Management Platform.

REPORT GENERATED ON

February 6, 2023 • 12:46 AM

More at www.hivepro.com